# Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/FR05/000635

International filing date: 16 March 2005 (16.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: FR
Number: 0403226
Filing date: 29 March 2004 (29.03.2004)

Date of receipt at the International Bureau: 27 May 2005 (27.05.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

R E P U B L I Q U E  F R A N Ç A I S E

PCT/FR2005/000635

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

# BREVET D'INVENTION

## CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

## COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 21 MARS 2005

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint-Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr

1er dépôt

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE
26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

# BREVET D'INVENTION
## CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11354*03

## REQUÊTE EN DÉLIVRANCE page 1/2

**BR1**

Cet imprimé est à remplir lisiblement à l'encre noire DB 540 e W / 210502

Réservé à l'INPI

REMISE DES PIÈCES DATE 29 MARS 2004
LIEU 69 INPI LYON
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0403226
DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 29 MARS 2004

**1** NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

Cabinet GERMAIN & MAUREAU
BP 6153
69466 LYON CEDEX 06

**Vos références pour ce dossier** *(facultatif)* GBR/ANT/045741

**Confirmation d'un dépôt par télécopie** ☐ N° attribué par l'INPI à la télécopie

**2** NATURE DE LA DEMANDE — Cochez l'une des 4 cases suivantes

| | |
|---|---|
| Demande de brevet | ☒ |
| Demande de certificat d'utilité | ☐ |
| Demande divisionnaire | ☐ |
| *Demande de brevet initiale* | N° Date |
| *ou demande de certificat d'utilité initiale* | N° Date |
| Transformation d'une demande de brevet européen *Demande de brevet initiale* | ☐ N° Date |

**3** TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Procédé de transmission d'un fichier de données numériques au travers de réseaux de télécommunications ou de radiocommunications

**4** DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE

Pays ou organisation Date N°
Pays ou organisation Date N°
Pays ou organisation Date N°

☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»**

**5** DEMANDEUR (Cochez l'une des 2 cases) ☐ Personne morale ☒ Personne physique

| | | |
|---|---|---|
| Nom ou dénomination sociale | | JOLIOT |
| Prénoms | | Philippe |
| Forme juridique | | |
| N° SIREN | | |
| Code APE-NAF | | |
| Domicile ou siège | Rue | Villa les Quatre Vents<br>Chemin de Gaujac |
| | Code postal et ville | 30130 PONT SAINT ESPRIT |
| | Pays | FRANCE |
| Nationalité | | Française |
| N° de téléphone *(facultatif)* | | N° de télécopie *(facultatif)* |
| Adresse électronique *(facultatif)* | | |

☐ **S'il y a plus d'un demandeur, cochez la case et utilisez l'imprimé «Suite»**

Remplir impérativement la 2ème page

1er dépôt

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

# BREVET D'INVENTION
## CERTIFICAT D'UTILITÉ

## REQUÊTE EN DÉLIVRANCE
page 2/2

**BR2**

Réservé à l'INPI

REMISE DES PIÈCES
DATE 29 MARS 2004
LIEU 69 INPI LYON

N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0403226

DB 540 W / 210502

| | | |
|---|---|---|
| **6 MANDATAIRE** *(s'il y a lieu)* | | |
| Nom | | |
| Prénom | | |
| Cabinet ou Société | | Cabinet GERMAIN & MAUREAU |
| N °de pouvoir permanent et/ou de lien contractuel | | |
| Adresse | Rue | BP 6153 |
| | Code postal et ville | 6 9 4 6 6 LYON CEDEX 06 |
| | Pays | FRANCE |
| N° de téléphone *(facultatif)* | | 04 72 69 84 30 |
| N° de télécopie *(facultatif)* | | 04 72 69 84 31 |
| Adresse électronique *(facultatif)* | | |
| **7 INVENTEUR (S)** | | **Les inventeurs sont nécessairement des personnes physiques** |
| Les demandeurs et les inventeurs sont les mêmes personnes | | ☒ Oui<br>☐ Non : **Dans ce cas remplir le formulaire de Désignation d'inventeur(s)** |
| **8 RAPPORT DE RECHERCHE** | | **Uniquement pour une demande de brevet (y compris division et transformation)** |
| Établissement immédiat ou établissement différé | | ☒<br>☐ |
| Paiement échelonné de la redevance *(en deux versements)* | | **Uniquement pour les personnes physiques effectuant elles-mêmes leur propre dépôt**<br>☐ Oui<br>☐ Non |
| **9 RÉDUCTION DU TAUX DES REDEVANCES** | | **Uniquement pour les personnes physiques**<br>☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)*<br>☐ Obtenue antérieurement à ce dépôt pour cette invention *(joindre une copie de la décision d'admission à l'assistance gratuite ou indiquer sa référence)* : AG |
| **10 SÉQUENCES DE NUCLEOTIDES ET/OU D'ACIDES AMINÉS** | | ☐ Cochez la case si la description contient une liste de séquences |
| Le support électronique de données est joint | | ☐ |
| La déclaration de conformité de la liste de séquences sur support papier avec le support électronique de données est jointe | | ☐ |
| **Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes** | | |

**11 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE**
**(Nom et qualité du signataire)**

Lyon, le 29 Mars 2004
Gérard BRATEL
CPI 921037

Gérard BRATEL
CPI 921037

**VISA DE LA PRÉFECTURE OU DE L'INPI**

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

La présente invention concerne un procédé de transmission sécurisée et confidentielle de données numériques au travers d'une architecture de réseaux multiples et indépendants de télécommunications ou de radiocommunications, qu'il s'agisse de données numériques statiques, c'est à dire enregistrées sur tout type de supports mémoires, ou dynamiques, c'est à dire non fixées sur de tels supports.

Il est généralement admis que le mode de communication entre deux points distants est un canal de transmission unique, dans lequel transite toute l'information selon un protocole de transmission tel que TCP/IP, IKE, IPsec, UDP, etc... Quel que soit le protocole choisi pour cette transmission, un bloc de données initial est acheminé dans sa totalité sous forme de paquets successifs au sein d'un canal unique. Par conséquent, l'information de ce bloc de données initial est accessible en totalité sur ce canal de transmission. Il n'existe donc pour une session de transmission de données entre deux points distants à un instant choisi qu'une unique convention de transmission "mono canal" supportée ensuite par un protocole quelconque. Ainsi, cette unicité de convention de transmission à l'instant choisi limite temporellement et physiquement la transmission.

La présente invention vise à éviter ces inconvénients en fournissant un procédé de transmission sécurisée et confidentielle de données numériques au travers d'une architecture de réseaux multiples et indépendants de télécommunications ou de radiocommunications, dans lequel l'information initiale n'est pas accessible en totalité durant sa transmission, et permettant de choisir à un instant donné une convention de transmission parmi une multitude de conventions très largement supérieure au nombre que permettrait un simple hachage d'un bloc initial de données en sous-unités élémentaires adressées ensuite vers des relais de transmission intermédiaires, puis ré-acheminées vers un destinataire final.

A cet effet, l'invention a essentiellement pour objet un procédé de transmission sécurisée et confidentielle d'un fichier de données numériques entre un élément expéditeur et un élément destinataire au travers de réseaux de télécommunications ou de radiocommunications, dans lequel :

- l'élément expéditeur télédécharge d'une base de données répertoriant les éléments expéditeurs autorisés, une clé secrète symétrique de fragmentation-transmission ;

- l'élément expéditeur transmet la clé de fragmentation-transmission à l'élément destinataire par l'intermédiaire d'un relais dit de deuxième niveau ;

- le relais de deuxième niveau informe la base de données que la clé de fragmentation-transmission est en cours d'utilisation ;

- l'élément destinataire transmet à l'élément expéditeur une autorisation d'envoi des fragments par l'intermédiaire du relais de deuxième niveau ;

- l'élément expéditeur fragmente les données du fichier initial, selon une distribution incrémentale avant attribution par permutation, de sorte que les données de chaque fragment sont inintelligibles, le niveau de fragmentation et le type de fragmentation étant prédéfinis dans la clé de fragmentation-transmission ;

- l'élément expéditeur attribue à chaque fragment un chemin d'adressage au travers d'un réseau de relais dits de premier niveau ;

- l'élément expéditeur transmet chaque fragment à l'élément destinataire via les relais de premier niveau ;

- l'élément destinataire réassemble, d'après les instructions de la clé de fragmentation-transmission, les fragments reçus pour recréer le fichier de données initial ;

- l'élément destinataire envoie un accusé de réception et de contrôle du réassemblage du fichier initial à la base de données par l'intermédiaire du relais de deuxième niveau ;

- la clé de fragmentation-transmission est supprimée de la base de données.

Ainsi, l'idée inventive consiste à réaliser une dissémination multi-temporelle et multi-spatiale non orthodromique de toutes données préalablement fragmentées par l'élément l'expéditeur, la transmission des fragments créés dans une architecture de réseaux de relais multiples et indépendants, à destination d'un ou plusieurs éléments destinataires distants qui effectuent un ré-assemblage des éléments transmis, permettant la reconstitution des données initiales dans leur forme originale.

Il est avantageusement défini plusieurs classes différentes permettant de définir l'objet information initiale à transmettre, à savoir:

- une classe T de types de fragmentation du genre bits à bits, octets à octets, bloc d'octets à bloc d'octets, bloc de bits à bloc de bits, espace

à espace (par exemple saut de caractère à saut de caractère, d'une harmonique de fréquence à la réapparition de la même harmonique de fréquence, d'un signal électromagnétique à la réapparition du même signal électromagnétique), et donc toutes les instances possibles et imaginables pour chacun des types précités ;

- une classe F de niveau de fragmentation, F étant un entier réel au moins égal à deux déterminé lors du choix de niveau de fragmentation ;

- une classe R de taille de réseaux, R étant un entier réel au moins égal à un, et de préférence supérieur ou égal à deux, déterminé lors du choix de la taille de l'architecture réseaux ;

- une classe A d'adresses IP des relais de l'architecture réseaux de types adresses IP des relais dits de premier niveau, adresses IP des relais dits de deuxième niveau, avec toutes les instances possibles et imaginables que l'on peut supposer.

Le principe de l'invention est ainsi d'implémenter dans un premier temps les caractéristiques suivantes:

- taille R d'une architecture de réseaux de R relais de premier niveau indépendants (à adresse IP différentes) fonctionnant en parallèle ;

- caractéristique d'un relais indépendant (à adresse IP unique) affecté uniquement à la transmission de la convention d'échange entre la source et la destination ;

- niveau F de fragmentation du message original par création de F fichiers dans lesquels les éléments constitutifs du message original sont distribués par permutation ;

ce dans un système de génération de clés symétriques toutes uniques dans leur représentation, et ne permettant la transmission que pour l'architecture réseaux ci-dessus décrite.

Puis les données de chacune de ces clés prises une à une (considérée comme une suite d'instructions) sont implémentées dans un programme logiciel de fragmentation et d'expédition chargé de générer à partir d'une information initiale, les éléments à transmettre. Enfin, les données de la clé unique sont implémentées après sa transmission dans l'architecture réseaux dans un programme logiciel de réception et d'assemblage, chargé de réaliser les instructions de la clé transmise , et d'obtenir à partir des éléments transmis et reçus l'information initiale , tout en ayant satisfait aux conditions de signature et d'authentification de la transmission.

Selon la taille de l'architecture réseaux de relais indépendants de premier niveau utilisée, le niveau de fragmentation et le type de fragmentation (par exemple bits à bits, octets à octets, bloc d'octets à bloc d'octets, bloc de bits à bloc de bits, espace à espace...) du bloc de données initiales originales avant transmission, il est ainsi possible de générer de fait une infinité théorique de clés de fragmentation-transmission pour un même bloc de données initiales originales entre deux entités distantes.

Dans un mode de réalisation préféré de l'invention, la clé de fragmentation-transmission est composée de deux sous-clés, dont :

- une sous-clé de fragmentation-réassemblage, unique pour chaque fichier de données initial à transmettre, et dont les possibilités de dénombrement sont issues du calcul factoriel, comprenant les instructions nécessaires à la déstructuration du fichier de données initial et à la distribution par permutation dans un jeu de fragments ;

- une sous-clé d'expédition, unique pour chaque fichier de données initial à transmettre, et dont les possibilités de dénombrement sont issues du calcul exponentiel, comprenant des instructions nécessaires, telles que les adresses IP des relais de premier niveau, à l'acheminement des fragments au sein du réseau de relais de premier niveau.

Selon une possibilité, l'élément destinataire adresse une requête aux relais de premier niveau, dont l'adresse IP est contenue dans la sous-clé d'expédition, pour télédécharger les fragments. La réalisation d'une session de transmission peut ainsi être différée dans le temps tant que l'architecture réseaux reste pérenne et le droit à l'utilisation de la clé de fragmentation-transmission valide, ce qui assure une fonction d'archivage confidentiel et physiquement sécurisé.

Chacun des relais dits de premier niveau est avantageusement pourvu de moyens de gestion de reconnaissance des fragments entrants, de tri intelligent et de ré-expédition des mêmes fragments vers leur destinataire.

Le relais de deuxième niveau n'est de préférence pas relié au réseau de relais de premier niveau. Il est cependant possible, par exemple, que le relais de deuxième niveau appartienne au réseau de relais de premier niveau.

Selon le degré de confidentialité souhaité, le réseau de relais de premier niveau peut être asservi au relais de deuxième niveau pour la définition de certaines tâches de réadressage.

Il est envisageable qu'un relais de premier ou de deuxième niveau soit remplacé par trois relais en ligne dont le relais intermédiaire est une adresse IP reliée aux deux autres relais par une connexion non Internet.

Dans son ensemble, le procédé selon l'invention est compatible avec tout type de cryptographie ou de compression intervenant en aval ou en amont.

L'invention prend donc dans son principe le contre-pied du préjugé actuellement admis selon lequel, pour communiquer une information entre deux points distants, ne peut être utilisée qu'une voie unique de communication qui achemine la totalité de l'information.

L'invention permet de créer une infinité de réseaux à fonctionnement de type Internet à accès autorisé, dans lesquels les informations sont échangées de façon sécurisée et confidentielle. Chaque réseau de cette infinité de réseaux a un accès autorisé à la session de transmission, la durée d'une session pouvant être limitée au traitement et à la transmission d'une information, ou préétablie conjointement par le fournisseur du procédé et l'utilisateur.

Les techniques actuelles de cryptologie font appel soit à des méthodes de cryptage dites asymétriques à clé publique et clé privée (par exemple DES, triple DES, RSA...) soit à des méthodes dites à clé symétrique secrète (regroupant stéganographie, technique de masquage, techniques de transformation-permutation...), qui présentent toutes, d'un point de vue cryptologique, la faille suivante : quelle que soit la puissance du moyen de crypte utilisé, l'information initiale originale est accessible dans sa totalité et sera donc totalement intelligible dès réussite de l'attaque cryptanalytique .

D'un point de vue cryptologique, le procédé selon l'invention élimine cette faille, l'information originale totale étant déstructurée avant sa transmission (ou sa sauvegarde sur support mémoire), et n'étant donc jamais accessible en totalité pendant sa transmission (ou sa sauvegarde). L'information totale originale ne sera réintelligible que si tous les fragments sont récupérés, ce qui est rendu quasiment impossible par la dissémination multi-temporelle et multi-spatiale, cette récupération de tous les fragments étant une condition indispensable avant tout essai de clé dans le cas d'une attaque cryptanalytique.

De toute façon, l'invention sera bien comprise à l'aide de la description qui suit, en référence au dessin schématique annexé représentant un mode de mise en œuvre du procédé selon l'invention, sur lequel :

- la figure 1 est un schéma illustrant les architectures de réseaux employées ;
- la figure 2 est un schéma illustrant la structure d'une sous-clé de fragmentation-réassemblage ;
- la figure 3 est un schéma illustrant la structure d'une sous-clé d'expédition ;
- la figure 4 est un schéma illustrant la structure d'une clé de fragmentation-transmission ;
- la figure 5 illustre un exemple de session de transmission.

Comme l'indique le schéma de la figure 1, l'architecture réseaux est composée de deux réseaux parallèles indépendants.

Un premier réseau est constitué d'un relais 10, dit de "deuxième niveau", dont la fonction unique est d'assurer la transmission, entre un expéditeur 20 unique et un destinataire 30 distant, des seules données d'une clé de fragmentation-transmission, dit fichier CFT, et garantissant l'unicité d'autorisation de transmission de la clé CFT pré-choisie, échangée entre l'expéditeur et son destinataire.

Ce relais 10 de deuxième niveau est indépendant d'un réseau de R relais indépendants 40, 41, 42 à adresses IP pré-dédiées, dits de "premier niveau", dont la fonction unique est de transmettre uniquement entre l'expéditeur 20 et le destinataire 30 les fragments issus de la fragmentation et les données d'adressage propres à chacun de ces fragments. Chacun des R relais 40, 41, 42 de premier niveau est pourvu d'un logiciel de gestion de reconnaissance des fragments entrants, de tri intelligent et de ré-expédition des mêmes fragments vers leur destinataire 30 pré-défini.

Le fichier CFT est une clé secrète symétrique unique pour chaque transmission, pré-fournie au dispositif pour chaque bloc de données initial original traité. Il a une structure univoque à deux sous-clés, et sa taille totale est une variable sous dépendance de la taille R de l'architecture de réseaux choisie et du niveau F de fragmentation appliquée.

Une première sous-clé A dite de fragmentation-réassemblage comprend toutes les instructions nécessaires à la déstructuration du fichier initial original et à sa distribution dans un jeu de F fragments. Les éléments

issus de la destructuration du fichier initial original sont distribués dans ces fragments selon une loi de permutation dont les capacités sont issues des équations du calcul factoriel.

Une seconde sous-clé B dite d'expédition comprend toutes les instructions nécessaires à l'acheminement des F fragments au sein du réseau des relais de premier niveau.

Un logiciel de fragmentation et d'expédition LFE hébergé chez l'expéditeur 20 reçoit les instructions du fichier CFT pour réaliser d'une part la fragmentation du message original initial en F fragments, dont chacun a une taille environ F fois plus petite que la taille du message initial original traité. Par exemple, pour un message initial de 20 Ko et une fragmentation de niveau F = 100 en mode octet par octet, il y a 100 fragments de taille 200 octets ; de même pour un message initial original de très grande taille de 5 Gigaoctets et une fragmentation de taille 200, il y a 200 sous-fichiers d'une taille d'environ 25 Mo chacun.

Le logiciel LFE assure ensuite l'expédition de chacun des fragments selon les instructions de la sous-clé B, vers le destinataire 30, prédéfini par l'expéditeur 20, via le réseau de relais indépendants 40, 41, 42 de premier niveau, après avoir au préalable adressé au destinataire 30 prédéfini le fichier CFT, via le relais 10 de deuxième niveau, indépendant du réseau de relais de premier niveau. La distribution des F fragments au sein du réseau de relais 40, 41, 42 de premier niveau est régie par une combinaison des lois de permutation issues des équations du calcul factoriel et des lois de distribution des éléments d'un ensemble de F éléments dans un ensemble de R éléments. Chacun des F fragments n'est accompagné que de la partie d'adressage au sein de l'architecture réseaux le concernant.

Un logiciel de réception et d'assemblage dit LRA hébergé chez le destinataire reçoit les données du fichier CFT adressées via le relais 10 de deuxième niveau, instructions qui après comparaison avec la somme de certaines des données pertinentes acheminées avec les F fragments, permettront au logiciel LRA de réaliser le ré-assemblage des fragments arrivés au destinataire 30 via le réseau de relais 40, 41, 42 de premier niveau pour recréer le bloc de données initial original, selon les instructions du fichier CFT.

Le fichier CFT a une taille et un contenu définis par le paramètre R de taille de l'architecture réseaux et le niveau de fragmentation F choisi pour le procédé. En conséquence il y a lien d'interdépendance entre le fichier CFT et

l'architecture de réseaux. L'ensemble des fichiers CFT d'un réseau n'a de fonction et d'existence que pour l'architecture de réseaux pour lequel il a été conçu et en conséquence la transmission d'un fichier traité par le logiciel de fragmentation LFE ne pourra se faire que par l'architecture de réseaux considérée et ne pourra aboutir à un destinataire 30 que parce que la transmission a été autorisée dans l'architecture de réseaux. L'existence du fichier CFT affecté à un fichier informatique empêche son télé-déchargement à un destinataire quelconque si la transmission n'a pas été autorisée dans l'architecture de réseaux considérée, et le ré-assemblage impossible si la transmission a été réalisée ailleurs que dans cette architecture réseaux.

Les fragments, les sous-clés A et B, le fichier CFT sont conformes avec tout type de protocoles de transmission existant.

Les valeurs possibles de R et de F pour un type T (variable au sein d'un ensemble de constantes de type de fragmentation, prédéfinie avant application de la méthode de fragmentation) prédéfini ne sont théoriquement limitées que par la taille du bloc de données initial original, et permettent une infinité théorique de conventions d'échanges au sein de l'architecture de réseaux entre l'expéditeur et le destinataire. Les lois mathématiques de dénombrement permettent de calculer le nombre de conventions d'échanges pour R et F fixés et T prédéfini comme étant égal à $[(F!)^2.R^F]$.

Bien entendu, chaque fragment issu de la fragmentation d'un bloc de données peut être lui-même considéré comme un nouveau bloc de données original et subir à son tour une fragmentation supplémentaire.

Le nombre de conventions d'échanges différentes permis par le procédé, pour la transmission d'un fichier original entre un expéditeur et un destinataire, est de $[(F!)^2.R^F]$ pour des valeurs élevées de R et de F.

Toutes les données créées peuvent supporter l'application d'une méthode de cryptage de type chiffrage asymétrique avec clé publique et clé privée.

Il est par exemple possible de définir un nombre N de clés CFT actives pour une période de temps D, permettant de rendre confidentielles toutes les transmissions d'un réseau wifi pendant la période D considérée.

Le procédé selon l'invention est mis en œuvre comme suit.

Le logiciel LFE applique d'abord une fragmentation dite de niveau F au fichier original initial à transmettre, c'est-à-dire qu'il scinde les données du fichier initial original de façon incrémentale en n sous-unités élémentaires de

taille prédéfinie par le type de fragmentation (espace à espace, bit à bit, octet à octet, bloc de bits à bloc de bits, ou bloc d'octets à bloc d'octets), pour créer ainsi F groupes de sous-unités élémentaires le plus équitablement réparties.

Un indice issu de la sous-clé de fragmentation-réassemblage, dont les possibilités de dénombrement sont issues du calcul factoriel, est associé à chaque groupe des sous-unités élémentaires suscitées.

Un chemin de transmission au sein d'une architecture de réseaux de R relais intermédiaires entre l'expéditeur et le destinataire est attribué à chacun des F fragments créés. Les possibilités de dénombrement issues de cette architecture sont celles du calcul exponentiel.

Le logiciel LRA réassemble les F fragments après leur réception chez le destinataire 30 selon les données pertinentes du fichier CFT déjà acquises.

Les figures 2 à 4 représentent la structure du fichier CFT.

Dans l'exemple de fragmentation de la figure 2, exemple donné à titre didactique pour un type de fragmentation espace par espace et un niveau de fragmentation de 10, la sous-clé A est composée d'un tableau d'entiers qui à chaque fragment SF (sous-fichier) associe respectivement le énième mot du fichier original.

Soit "i" l'incrément dans le fichier "ici du premier au dernier mot de la liste", i+1M SF9 est : le $i^{ème}$ mot du texte va dans le sous-fichier SF9.

Ainsi, pour le texte suivant : "Les routeurs sont des dispositifs permettant de choisir le chemin que les datagrammes vont emprunter pour arriver à destination. Le routage est donc le processus qui consiste à définir le chemin que vont parcourir les données d'un ordinateur A jusqu'à un ordinateur B.", le fragment SF1 est "Les que routage chemin un" et le fragment SF3 est "sont datagrammes donc vont B."

Dans l'exemple de structure de sous-clé B de la figure 3, Adr désigne l'adresse IP des relais de premier niveau 40, 41, 42. Ici, seuls sont utilisés les relais Adr4, Adr6 et Adr9.

L'exemple des figures 2 et 3 est repris en figure 4 pour représenter la structure du fichier CFT (sous-clé A + sous-clé B).

Ainsi, la lecture de cette clé CFT se fait de la façon suivante :

- pour la sous-clé A :

Le ($1^{er}$, $11^{e}$, $21^{e}$, $31^{e}$...) mot va dans le fragment SF9 ;

Le ($2^{e}$,$12^{e}$, $22^{e}$, $32^{e}$ ...) mot va dans le fragment SF3 ;

Le ($3^e$,$13^e$, $23^e$, $33^e$ ...) mot va dans le fragment SF5 ;
Le ($4^e$,$14^e$, $24^e$, $34^e$ ...) mot va dans le fragment SF6 ;
Le ($5^e$,$15^e$, $25^e$, $35^e$ ...) mot va dans le fragment SF8 ;
Le ($6^e$,$16^e$, $26^e$, $36^e$ ...) mot va dans le fragment SF1 ;
Le ($7^e$,$17^e$, $27^e$, $37^e$ ...) mot va dans le fragment SF10 ;
Le ($8^e$,$18^e$, $28^e$, $38^e$ ...) mot va dans le fragment SF2 ;
Le ($9^e$,$19^e$, $29^e$, $39^e$ ...) mot va dans le fragment SF4 ;
Le ($10^e$, $20^e$, $30^e$, $40^e$ ...) mot va dans le fragment SF7.

- pour la sous-clé B :

Les $1^e$, $2^e$, et $8^e$ fragments (SF8, SF1, SF2) passent par le relais dont l'adresse IP est la $4^e$ de la série ; les $4^e$, $5^e$, $7^e$ et $10^e$ fragments (SF4, SF5, SF7, SF10) passent par le relais dont l'adresse IP est la $6^e$ de la série ; les $3^e$, $6^e$ et $9^e$ fragments (SF3, SF6, SF9) passent par le relais dont l'adresse IP est la $9^e$ de la série.

Le schéma de la figure 5 illustre un exemple de session de transmission, dont les étapes sont les suivantes.

- étape S1 : l'expéditeur 20 fait une demande d'attribution de clé CFT. S'il est déjà client répertorié dans la base de données 50 et possesseur d'un lot de clés réservées, sa demande est transmise à la base de données 50. S'il est déjà client mais non possesseur d'un lot de clés réservées, sa demande est traitée par des logiciels d'arrière guichet de site web (non représentés) avant d'être transmise à la base de données 50. Enfin, s'il n'est pas client, sa demande est traitée par les logiciels d'arrière guichet de site web avant d'être transmise à la base de données 50 (soit achat d'une clé, soit achat d'un lot de clés réservées). La demande est donc transmise à la base de données 50 qui extrait une clé CFT soit disponible à partir du lot de clés CFT réservées, soit disponible en dehors des lots de clés CFT réservées
- étape S2 : La clé CFT choisie par la base de données 50 est téléchargée vers le client expéditeur 20.
- étape S3 : La clé CFT est adressée par le logiciel LFE dans la trame CFT vers le relais 10 de deuxième niveau.
- étape S4 : Le relais 10 de deuxième niveau informe la base de données 50 que la clé CFT est en cours d'utilisation et ne doit donc plus être attribuée mais pas encore éliminée de la base de données 50.
- étape S5 : Le relais 10 de deuxième niveau tente de se connecter au destinataire 30 pour lui adresser la trame Email CFT.

Si le destinataire 30 est connecté, la trame Email CFT est reçue dans le logiciel LRA et un message d'autorisation d'envoi des trames fragments finalisées avec leur donnée pertinente d'adressage dans le réseau 40, 41, 42 est élaboré.

Si le destinataire 30 n'est pas connecté, la trame Email CFT reste dans le relais 10 de deuxième niveau et la procédure de transmission est suspendue. Le destinataire 30 devra venir chercher au relais 10 de deuxième niveau la trame Email CFT comme cela se fait actuellement pour un Email. Il faut cependant s'assurer que personne ne peut se substituer au destinataire 30 en vérifiant par exemple son adresse IP.

- étape S6 : Le message d'autorisation d'envoi des trames fragments est transmis au relais 10 de deuxième niveau qui est le seul à connaître l'adresse IP de l'expéditeur 20 de la trame CFT concernée.

- étape S7 : Le relais 10 de deuxième niveau adresse à l'expéditeur 20 le message d'autorisation d'envoi des trames fragments.

Si l'expéditeur 20 est connecté, le message d'autorisation d'envoi active l'expédition vers les relais 40, 41, 42 de premier niveau des fragments créés auparavant. Si l'expéditeur 20 n'est pas connecté, il reçoit un message lui demandant de se connecter, Il devra alors venir chercher le message d'autorisation d'envoi.

- étape S8 : Les trames fragments sont expédiées vers les relais 40, 41, 42 de premier niveau.

- étape S9 : Les trames fragments sont réexpédiées par les relais 40, 41, 42 de premier niveau.vers le destinataire 30. Si le destinataire 30 est connecté la procédure se poursuit.

Si le destinataire 30 n'est plus connecté, les relais 40, 41, 42 de premier niveau informent le destinataire 30 de se connecter et procédent à une nouvelle tentative de connexion puis d'expédition des trames fragments ; un nombre maximum de tentatives de connexion-expédition avec un temps maximum autorisé raisonnable est prédéterminé. En ce cas le destinataire 30 ne peut en aucun cas chercher les trames fragments qui lui sont destinées chez les relais de premier niveau 40, 41, 42.

Le logiciel de réception-assemblage LRA du destinataire 30 peut générer, à partir des données du fichier CFT, des « Email requêtes » avec comme adresses de destination les adresses IP des relais 40, 41, 42 de premier niveau contenues dans la sous-clé B du fichier CFT, permettant de

récupérer au niveau de chaque relais 40, 41, 42 de premier niveau concerné, uniquement les trames fragments identifiées comme appartenant à la session de transmission du bloc de données initial original.

- étape S10 : Le destinataire 30 envoie au relais 10 de deuxième niveau un accusé de réception du type ICV "Integrity Check Value" (mot de contrôle) du message assemblé. L' ICV contenue dans la trame CFT (donc du message total initial) indique que l'assemblage est réussi.

- étape S11 : Cet accusé de réception valide donc la totalité de la session et est transmis à la base de données 50 pour sortir définitivement la clé CFT utilisée de la liste des clés CFT disponibles.

Les trois paramètres R (variable de taille de d'architecture réseaux de premier niveau), F (variable de niveau de fragmentation), T (variable au sein d'un ensemble de constantes de type de fragmentation, prédéfinie avant application de la méthode de fragmentation) sont indissociables entre eux, c'est-à-dire que l'existence de l'un entraîne l'existence des deux autres, mais ils peuvent prendre des valeurs différentes les uns des autres.

La conjugaison de ces trois paramètres définit la plate-forme des fonctions et des propriétés potentielles de l'application du procédé ci-dessus décrit. Les possibilités du choix de la valeur de chacun de ces trois paramètres permettent d'obtenir la prééminence de l'une ou plusieurs des fonctions et des propriétés potentielles de l'application du procédé, et donc de définir un ensemble de services de transmission aux propriétés principales notablement différentes et pré-orientées vers la fonction ou la propriété principale désirée. Il faut noter que la modulation par exemple du paramètre R, entier réel au moins égal à 2, est intéressante : plus R est bas pour F donné, moins le coût de transmission est élevé ; plus R est grand pour F donné, plus le coût de transmission est grand, mais plus la sécurité et la confidentialité de transmission sont élevées.

L'ensemble de ces fonctions liées mais à lien de dépendance variable entre elles, coexistantes dès la mise en application du procédé peuvent se répartir en deux groupes.

Un premier groupe rassemble les fonctions systématiquement présentes et non modulées par la variation d'un des trois paramètres F, R et T. Ces fonctions sont :

- d'autoriser sur l'architecture du réseau uniquement les fragments créés par le procédé, et d'interdire l'acheminement sur le réseau et donc la

réception chez un quelconque destinataire non reconnu et autorisé de toute autre donnée non traitée par le procédé ;

- d'assurer la protection des données enregistrées sur un support de stockage (par exemple CD, SACD, DVD, mémoire) et d'interdire la transmission et le télé-déchargement non autorisés dans un environnement adéquat ;

- de diminuer l'infectivité et la contagiosité de tout virus (sans pouvoir être exporté vers de multiples destinataires) à partir du moment où toute transmission sur l'architecture du réseau est rendue unique par l'attribution d'un fichier CFT unique, et que tout fichier potentiellement porteur d'un virus ne peut être infectant qu'après ré-assemblage et exécution ;

- de limiter l'ampleur du pollupostage ;

- d'assurer la non répudiation des données.

Un second groupe rassemble les fonctions systématiquement présentes mais dont la prééminence et la puissance peuvent être modulées par la variation de l'un ou plusieurs des paramètres F,R et T. Ces fonctions sont :

- d'assurer l'échange confidentialisé des données transmises après application du procédé ;

- d'assurer un moyen cryptologique puissant (théoriquement illimité) et de fait limité que par la taille du bloc de données initial à traiter ;

- de rendre possible la transmission de données sans limite théorique de taille autre que celle imposée par la taille physique du réseau et le niveau de fragmentation , sans augmenter significativement le temps de transmission ;

- de transmettre de façon cryptée tout type de données sans augmentation significative de taille des données initiales ;

- de sauvegarder et d'archiver de façon cryptée tout type de données.

Comme il va de soi, l'invention ne se limite pas au seul mode de mise en oeuvre décrit ci-dessus à titre d'exemple ; elle en embrasse au contraire toutes les variantes. Ainsi, il est envisageable d'utiliser ce procédé dans une application d'archivage et de sauvegarde sécurisée et confidentielle de données sur tout type de support mémoire (CD, SACD, DVD, SuperDVD, etc...).

## REVENDICATIONS

1 - Procédé de transmission sécurisée et confidentielle d'un fichier de données numériques entre un élément expéditeur et un élément destinataire au travers de réseaux de télécommunications ou de radiocommunications, caractérisé en ce que :

- (étapes S1, S2) l'élément expéditeur (20) télédécharge d'une base de données (50) répertoriant les éléments expéditeurs autorisés, une clé (CFT) secrète symétrique de fragmentation-transmission ;
- (étapes S3, S5) l'élément expéditeur (20) transmet la clé de fragmentation-transmission (CFT) à l'élément destinataire (30) par l'intermédiaire d'un relais (10) dit de deuxième niveau ;
- (étape S4) le relais (10) de deuxième niveau informe la base de données (50) que la clé de fragmentation-transmission (CFT) est en cours d'utilisation ;
- (étapes S6, S7) l'élément destinataire (20) transmet à l'élément expéditeur (30) une autorisation d'envoi des fragments par l'intermédiaire du relais (10) de deuxième niveau ;
- l'élément expéditeur (20) fragmente les données du fichier initial, selon une distribution incrémentale avant attribution par permutation, de sorte que les données de chaque fragment sont inintelligibles, le niveau et le type de fragmentation étant prédéfinis dans la clé de fragmentation-transmission ;
- l'élément expéditeur (20) attribue à chaque fragment un chemin d'adressage au travers d'un réseau de relais (40, 41, 42) dits de premier niveau;
- (étapes S8, S9) l'élément expéditeur (20) transmet chaque fragment à l'élément destinataire (30) via les relais (40, 41, 42) de premier niveau ;
- l'élément destinataire (30) réassemble, d'après les instructions de la clé de fragmentation-transmission (CFT), les fragments reçus pour recréer le fichier de données initial ;
- (étape S10) l'élément destinataire (30) envoie un accusé de réception et de contrôle du réassemblage du fichier initial à la base de données (50) par l'intermédiaire du relais (10) de deuxième niveau ;
- (étape S11) la clé de fragmentation-transmission (CFT) est supprimée de la base de données (50).

2 – Procédé selon la revendication 1, caractérisé en ce qu'il est défini plusieurs classes différentes permettant de définir l'objet information initiale à transmettre, à savoir:

- une classe T de types de fragmentation du genre bits à bits, octets à octets, bloc d'octets à bloc d'octets, bloc de bits à bloc de bits, espace à espace, et donc toutes instances possibles pour chacun des types précités ;
- une classe F de niveau de fragmentation, F étant un entier réel au moins égal à deux déterminé lors du choix de niveau de fragmentation ;
- une classe R de taille de réseaux, R étant un entier réel au moins égal à un, et de préférence supérieur ou égal à deux, déterminé lors du choix de la taille de l'architecture réseaux ;
- une classe A d'adresses IP des relais de l'architecture réseaux de types adresses IP des relais dits de premier niveau, adresses IP des relais dits de deuxième niveau, avec toutes instances possibles.

3 – Procédé selon la revendication 1 ou 2, caractérisé en ce que la clé de fragmentation-transmission (CFT) est composée de deux sous-clés, dont :

- une sous-clé (A) de fragmentation-réassemblage, unique pour chaque fichier de données initial à transmettre, et dont les possibilités de dénombrement sont issues du calcul factoriel, comprenant les instructions nécessaires à la destructuration du fichier de données initial et à la distribution par permutation dans un jeu de fragments ;
- une sous-clé (B) d'expédition, unique pour chaque fichier de données initial à transmettre, et dont les possibilités de dénombrement sont issues du calcul exponentiel, comprenant des instructions nécessaires, telles que les adresses IP des relais (40, 41, 42) de premier niveau, à l'acheminement des fragments au sein du réseau de relais (40, 41, 42) de premier niveau.

4 – Procédé selon la revendication 3, caractérisé en ce que l'élément destinataire (30) adresse une requête aux relais (40, 41, 42) de premier niveau, dont l'adresse IP est contenue dans la sous-clé (B) d'expédition, pour télédécharger les fragments.

5 – Procédé selon l'une des revendications 1 à 4, caractérisé en ce que chacun des relais (40, 41, 42) de premier niveau est pourvu de moyens de gestion de reconnaissance des fragments entrants, de tri intelligent et de ré-expédition des mêmes fragments vers leur destinataire (30).

6 – Procédé selon l'une des revendications 1 à 5, caractérisé en ce que le relais (10) de deuxième niveau n'est pas relié au réseau de relais (40, 41, 42) de premier niveau.

7 – Procédé selon l'une des revendications 1 à 5, caractérisé en ce que le réseau de relais (40, 41, 42) de premier niveau est asservi au relais (10) de deuxième niveau pour la définition de tâches de réadressage.

8 – Procédé selon l'une des revendications 1 à 7, caractérisé en ce qu'un relais de premier niveau (40, 41, 42) ou de deuxième (10) niveau est remplacé par trois relais en ligne dont le relais intermédiaire est une adresse IP reliée aux deux autres relais par une connexion non Internet.

FIG1

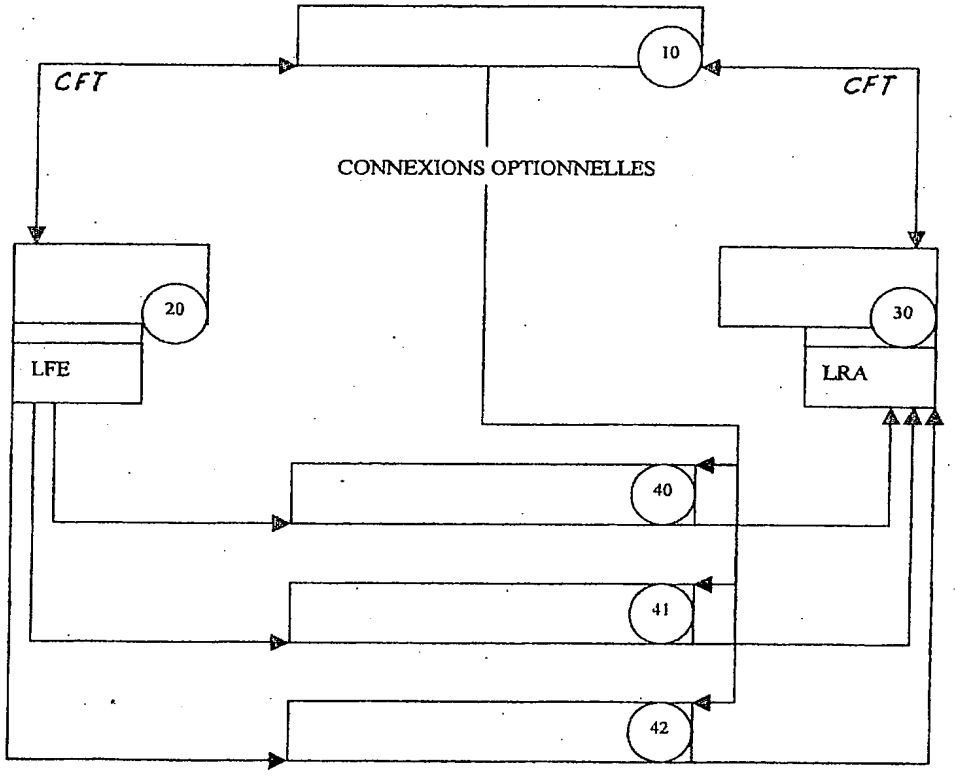

FIG5

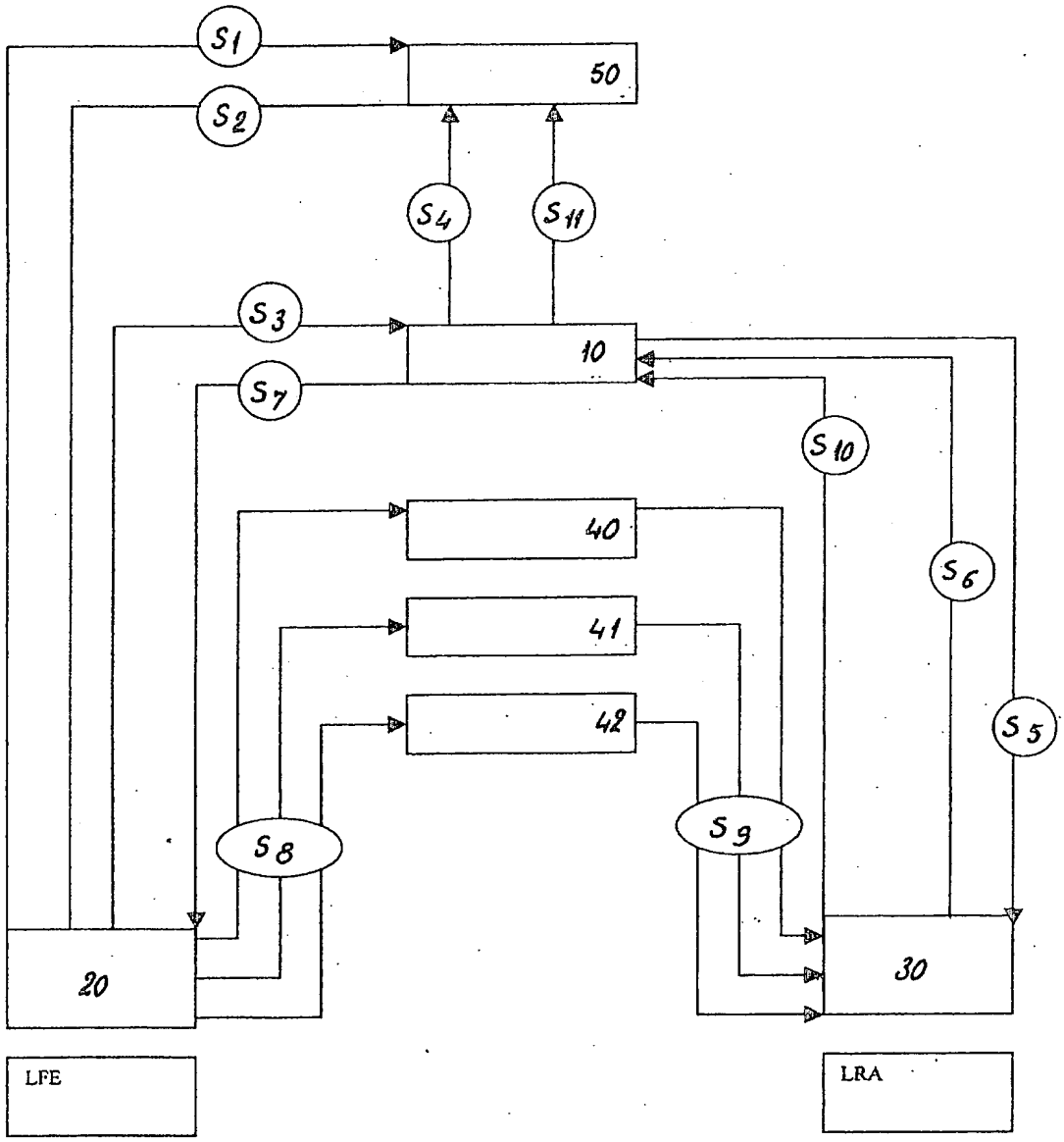

FIG2

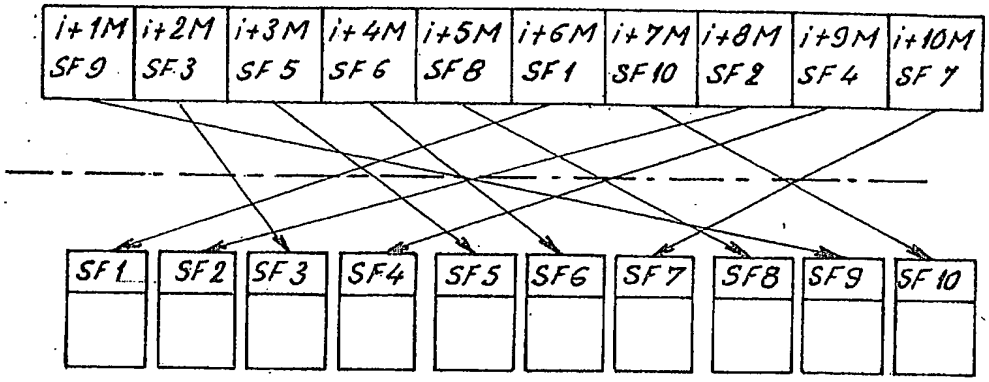


FIG3

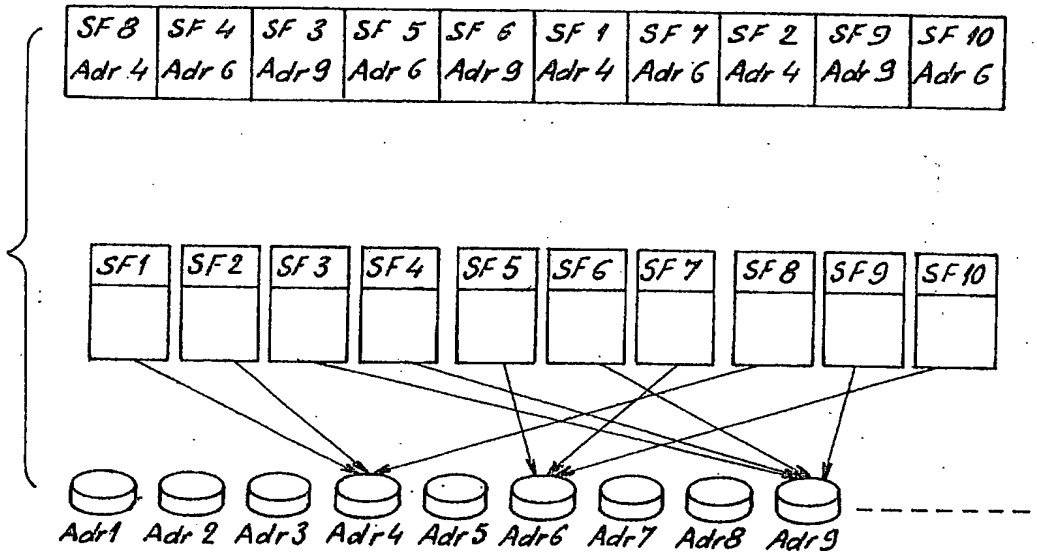


FIG4

Clé A + Clé B

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1/9 | 2/3 | 3/5 | 4/6 | 5/8 | 6/1 | 7/10 | 8/2 | 9/4 | 10/7 |
| 8/4 | 4/6 | 3/9 | 5/6 | 6/9 | 1/4 | 7/6 | 2/4 | 9/9 | 10/6 |